脆弱性対策情報データベース JVN iPedia に関する活動報告レポート

[2020 年第 1 四半期（1 月～3 月）]

脆弱性対策情報データベース JVN iPedia に関する活動報告レポートについて

本レポートでは、2020 年 1 月 1 日から 2020 年 3 月 31 日までの間に JVN iPedia で登録をした脆弱性対策情報の統計及び事例について紹介しています。

独立行政法人情報処理推進機構　セキュリティセンター

2020 年 5 月 13 日

目次

1. 2020 年第 1 四半期 脆弱性対策情報データベース JVN iPedia の登録状況

脆弱性対策情報データベース「JVN iPedia（ https://jvndb.jvn.jp/ ）」は、ソフトウェア製品に関する脆弱性対策情報を 2007 年 4 月 25 日から日本語で公開しています。システム管理者が迅速に脆弱性対策を行えるよう、1）国内のソフトウェア開発者が公開した脆弱性対策情報、2）脆弱性対策情報ポータルサイト JVN [(*1)] で公表した脆弱性対策情報、3）米国国立標準技術研究所 NIST [(*2)] の脆弱性データベース「NVD [(*3)]」が公開した脆弱性対策情報を集約、翻訳しています。

1-1. 脆弱性対策情報の登録状況

～脆弱性対策情報の登録件数の累計は 116,604 件～

2020 年第 1 四半期（2020 年 1 月 1 日から 3 月 31 日まで）に JVN iPedia 日本語版へ登録した脆弱性対策情報は右表の通りとなり、2007 年 4 月 25 日に JVN iPedia の公開を開始してから本四半期までの、**脆弱性対策情報の登録件数の累計は 116,604 件になりました**（表 1-1、図 1-1）。

また、JVN iPedia 英語版へ登録した脆弱性対策情報は右表の通り、累計で 2,132 件になりました。

表 1-1. 2020 年第 1 四半期の登録件数

	情報の収集元	登録件数	累計件数
日本語版	国内製品開発者	5 件	232 件
	JVN	184 件	9,061 件
	NVD	4,331 件	107,311 件
	計	4,520 件	116,604 件
英語版	国内製品開発者	4 件	230 件
	JVN	35 件	1,902 件
	計	39 件	2,132 件

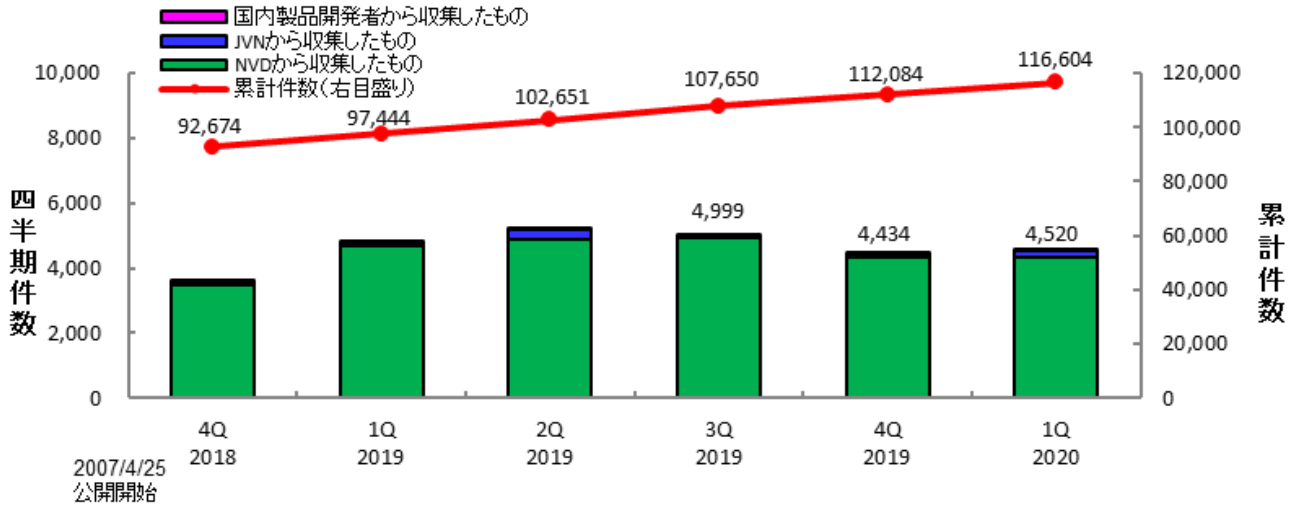

図 1-1. JVN iPedia の登録件数の四半期別推移

(*1) Japan Vulnerability Notes：脆弱性対策情報ポータルサイト。製品開発者の脆弱性への対応状況を公開し、システムのセキュリティ対策を支援しています。IPA、JPCERT/CC が共同で運営しています。 https://jvn.jp

(*2) National Institute of Standards and Technology：米国国立標準技術研究所。米国の科学技術分野における計測と標準に関する研究を行う機関：https://www.nist.gov

(*3) National Vulnerability Database：NIST が運営する脆弱性データベース。https://nvd.nist.gov

2. JVN iPedia の登録データ分類

2-1. 脆弱性の種類別件数

図 2-1 は、2020 年第 1 四半期（1 月～3 月）に JVN iPedia へ登録した脆弱性対策情報を、共通脆弱性タイプ一覧(CWE)によって分類し、件数を集計したものです。

集計結果は件数が多い順に、CWE-79（クロスサイトスクリプティング）が 636 件、CWE-20（不適切な入力確認）が 310 件、CWE-200（情報漏えい）が 305 件、CWE-269（不適切な権限管理）が 290 件、CWE-787（境界外書き込み）が 195 件でした。最も件数の多かった CWE-79（クロスサイトスクリプティング）は、悪用されると偽のウェブページが表示されたり、情報が漏えいしたりするおそれがあります。

製品開発者は、ソフトウェアの企画・設計段階から、脆弱性の低減に努めることが求められます。IPA ではそのための資料やツールとして、開発者や運営者がセキュリティを考慮したウェブサイトを作成するための資料「**安全なウェブサイトの作り方**[*4]」や「**IPA セキュア・プログラミング講座**[*5]」、脆弱性の仕組みを実習形式や演習機能で学ぶことができる脆弱性体験学習ツール「**AppGoat**[*6]」などを公開しています。

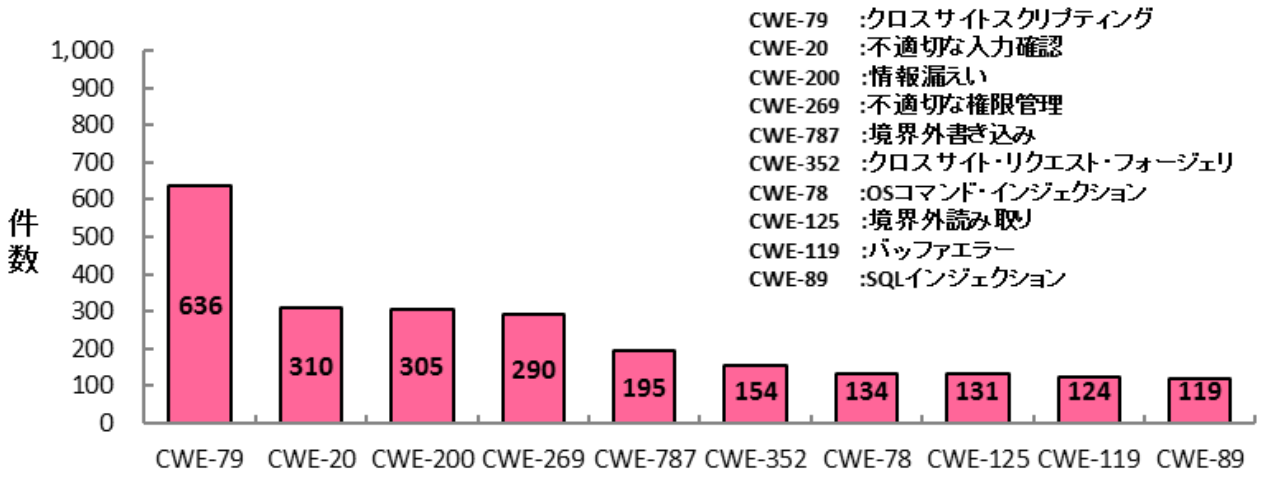

図 2-1. 2020 年第 1 四半期に登録された脆弱性の種類別件数

[*4] IPA：「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity.html

[*5] IPA：「IPA セキュア・プログラミング講座」
https://www.ipa.go.jp/security/awareness/vendor/programming/

[*6] IPA：脆弱性体験学習ツール 「AppGoat」
https://www.ipa.go.jp/security/vuln/appgoat/

2-2. 脆弱性に関する深刻度別割合

図 2-2 は JVN iPedia に登録済みの脆弱性対策情報を CVSSv2 の値に基づいて深刻度別に分類し、登録年別にその推移を示したものです。

2020 年に JVN iPedia に登録した脆弱性対策情報は深刻度別に、レベルⅢが全体の 25.2%、レベルⅡが 61.0%、レベルⅠが 13.8%となっており、情報の漏えいや改ざんされるような危険度が高い脅威であるレベルⅡ以上が 86.2%を占めています。

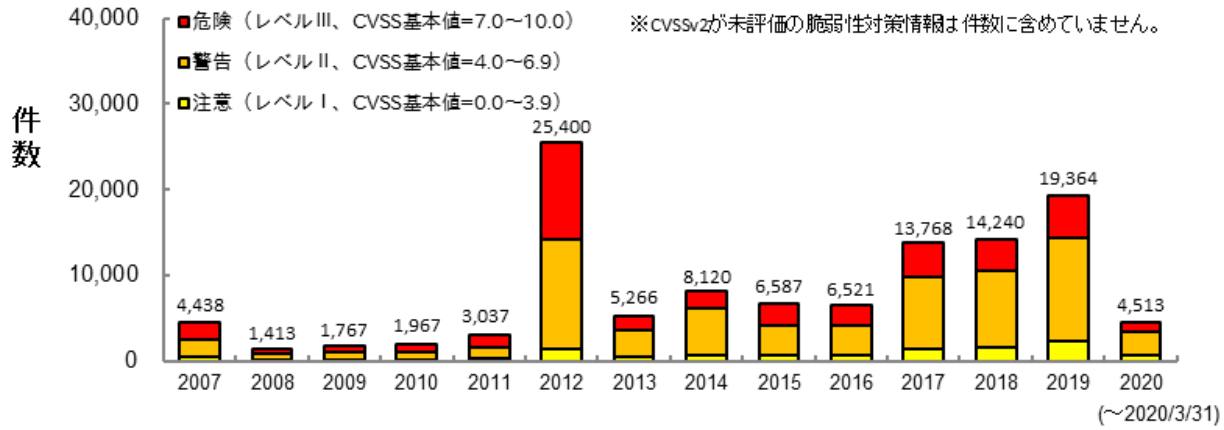

図 2-2. 脆弱性の深刻度別件数(CVSSv2)

図 2-3 は JVN iPedia に登録済みの脆弱性対策情報を CVSSv3 の値に基づいて深刻度別に分類し、登録年別にその推移を示したものです。

2020 年に JVN iPedia に登録した脆弱性対策情報は深刻度別に、「緊急」が全体の 16.2%、「重要」が 40.5%、「警告」が 41.8%、「注意」が 1.5%となっています。

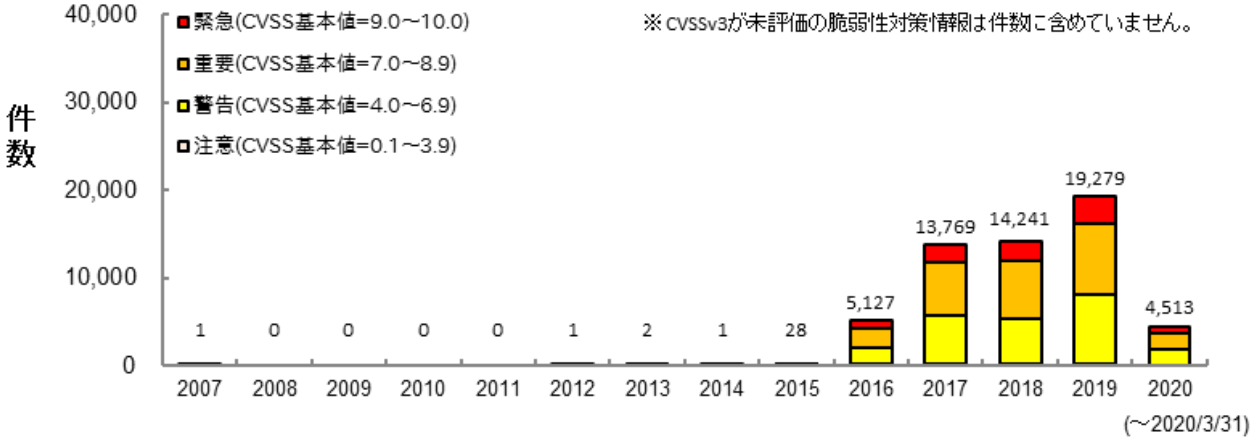

図 2-3. 脆弱性の深刻度別件数(CVSSv3)

既知の脆弱性による脅威を回避するため、製品開発者は常日頃から新たに報告される脆弱性対策情報に注意を払うと共に、**脆弱性が解消されている製品へのバージョンアップやアップデート**などを速やかに行ってください。

なお、新たに登録した JVN iPedia の情報を、RSS 形式や XML 形式 [*7] で公開しています。

[*7] IPA：データフィード
https://jvndb.jvn.jp/ja/feed/

2-3. 脆弱性対策情報を公開した製品の種類別件数

図 2-4 は JVN iPedia に登録済みの脆弱性対策情報をソフトウェア製品の種類別に件数を集計し、年次でその推移を示したものです。2020 年で最も多い種別は「アプリケーション」に関する脆弱性対策情報で、2020 年の件数全件の約 74.4%（3,362／全 4,519 件）を占めています。

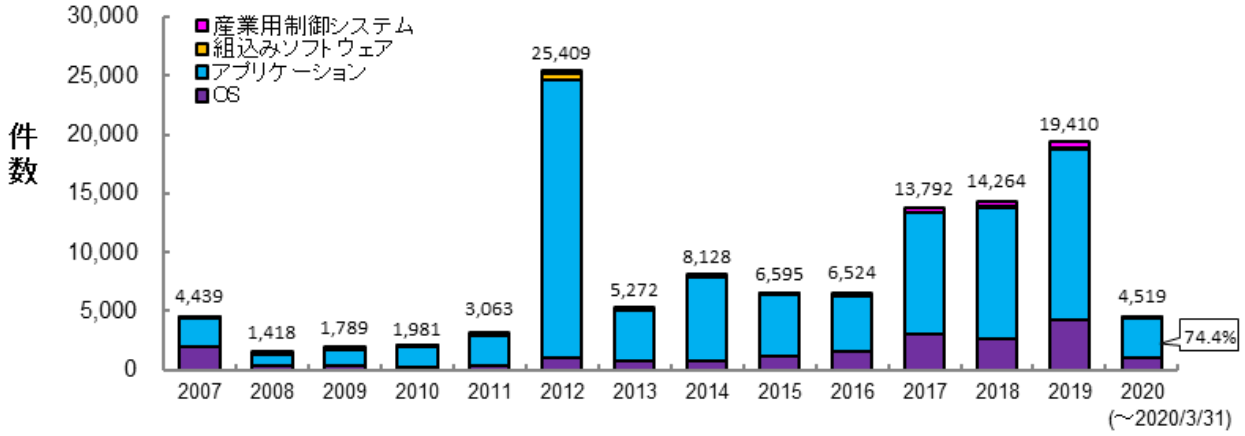

図 2-4. 脆弱性対策情報を公表した製品の種類別件数の公開年別推移

図 2-5 は重要インフラなどで利用される、産業用制御システムに関する脆弱性対策情報の件数を集計し、年次でその推移を示したものです。これまでに累計で 2,462 件を登録しています。

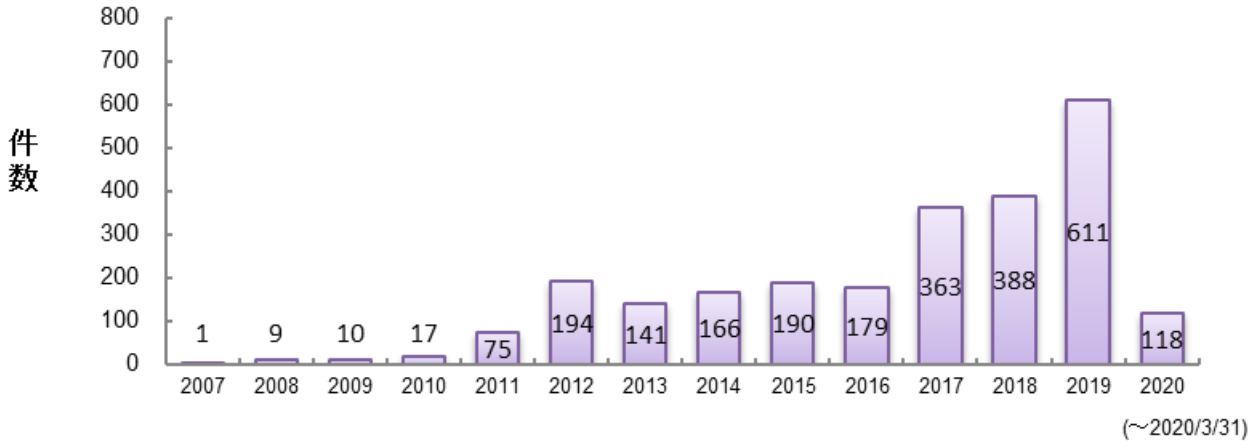

図 2-5. JVN iPedia 登録件数（産業用制御システムのみ抽出）

2-4. 脆弱性対策情報の製品別登録状況

表 2-1 は 2020 年第 1 四半期（1 月～3 月）に JVN iPedia へ登録された脆弱性対策情報の中で登録件数が多かった製品上位 20 件を示したものです。

本四半期において最も登録件数が多かったのは、マイクロソフトが提供する Microsoft Windows 10 でした。2 位以降も同社製品である Windows OS が多くランクインされています。他にもアップルが提供する iOS や Apple Mac OS X 等、OS 製品に関する脆弱性対策情報が多く登録されました。

JVN iPedia は、表に記載されている製品以外にも幅広い脆弱性対策情報を登録公開しています。製品の利用者や開発者は、自組織などで使用しているソフトウェアの脆弱性対策情報を迅速に入手し、効率的な対策に役立ててください [(*8)]。

表 2-1. 製品別 JVN iPedia の脆弱性対策情報登録件数　上位 20 件 [2020 年 1 月～2020 年 3 月]

順位	カテゴリ	製品名（ベンダ名）	登録件数
1	OS	Microsoft Windows 10 (マイクロソフト)	188
2	OS	Microsoft Windows Server (マイクロソフト)	182
3	OS	Microsoft Windows Server 2019 (マイクロソフト)	174
4	OS	Microsoft Windows Server 2016 (マイクロソフト)	165
5	OS	Microsoft Windows Server 2012 (マイクロソフト)	131
6	OS	Microsoft Windows 8.1 (マイクロソフト)	127
7	OS	Microsoft Windows RT 8.1 (マイクロソフト)	125
8	開発環境	GitLab (GitLab.org)	120
9	ナレッジベースソフトウェア	PHPKB (Chadha Software Technologies)	119
10	OS	Microsoft Windows Server 2008 (マイクロソフト)	105
11	OS	Microsoft Windows 7 (マイクロソフト)	103
12	OS	Android (Google)	81
13	ファームウェア	Qualcomm compornent (クアルコム)	71
14	OS	iOS (アップル)	53
15	ブラウザ	Google Chrome (Google)	50
16	OS	Apple Mac OS X (アップル)	48
17	OS	tvOS (アップル)	42
18	ブラウザ	Mozilla Firefox (Mozilla Foundation)	41
19	PDF 閲覧・編集	Adobe Acrobat DC (アドビシステムズ)	40
19	PDF 閲覧	Adobe Acrobat Reader DC (アドビシステムズ)	40

[(*8)] 脆弱性情報の収集や集めた情報の活用方法についての手引きをまとめたレポート
「脆弱性対策の効果的な進め方（実践編）」を公開。
https://www.ipa.go.jp/security/technicalwatch/20150331.html

3. 脆弱性対策情報の活用状況

表 3-1 は 2020 年第 1 四半期（1 月～3 月）にアクセスの多かった JVN iPedia の脆弱性対策情報の上位 20 件を示したものです。

1 位、2 位にランクインした Junos OS は企業向けルータ等で使用される OS 製品です。この製品に影響する脆弱性種別はクロスサイトスクリプティングとディレクトリトラバーサルとなっており、悪用された場合、ルータ管理者が操作するウェブ画面上で任意のスクリプトが実行されたり、サーバ上のファイルが閲覧・削除されたりする可能性があります。利用者は影響を受けるバージョンを確認し、必要に応じて最新版へのアップデートまたはワークアラウンドを実施し、攻撃による被害を未然に防ぐことが求められます。

表 3-1. JVN iPedia の脆弱性対策情報へのアクセス　上位 20 件 [2020 年 1 月～2020 年 3 月]

順位	ID	タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス数
1	JVNDB-2020-000003	Junos OS におけるクロスサイトスクリプティングの脆弱性	2.6	6.1	2020/1/10	7,342
2	JVNDB-2020-000002	Junos OS におけるディレクトリトラバーサルの脆弱性	5.5	5.4	2020/1/10	7,326
3	JVNDB-2020-000001	F-RevoCRM におけるクロスサイトスクリプティングの脆弱性	2.6	6.1	2020/1/8	7,250
4	JVNDB-2020-000005	トレンドマイクロ製パスワードマネージャーにおける情報漏えいの脆弱性	1.7	3.3	2020/1/17	6,569
5	JVNDB-2019-000074	Athenz におけるオープンリダイレクトの脆弱性	4.3	4.7	2019/12/12	6,089
6	JVNDB-2019-013271	Hitachi Automation Director における複数の脆弱性	なし	なし	2019/12/24	5,975
7	JVNDB-2019-000077	Android アプリ「日テレニュース 24」における SSL サーバ証明書の検証不備の脆弱性	4.0	4.8	2019/12/19	5,882
8	JVNDB-2020-000006	富士ゼロックス製の複数のスマートフォンアプリにおける SSL サーバ証明書の検証不備の脆弱性	4.0	4.8	2020/1/21	5,869
9	JVNDB-2019-000078	a-blog cms における複数の脆弱性	4.3	6.1	2019/12/20	5,868
10	JVNDB-2019-013273	Hitachi Compute Systems Manager における DoS 脆弱性	なし	なし	2019/12/24	5,732
11	JVNDB-2019-000058	複数のリコー製プリンタおよび複合機における複数のバッファオーバーフローの脆弱性	7.5	9.8	2019/9/13	5,429
12	JVNDB-2019-013272	Hitachi Command Suite 製品および Hitachi Infrastructure Analytics Advisor における複数の脆弱性	なし	なし	2019/12/24	5,407
13	JVNDB-2019-000076	サイボウズ Office における複数の脆弱性	4.0	7.7	2019/12/17	5,294
14	JVNDB-2019-011088	ウイルスバスターコーポレートエディションにおけるディレクトリトラバーサルの脆弱性	5.2	8.2	2019/10/29	5,271
15	JVNDB-2019-014437	リコー製プリンタドライバにおける権限昇格の脆弱性	4.3	7.8	2020/2/17	5,183

16	JVNDB-2020-000016	Aterm WF1200CR、WG1200CR および WG2600HS における複数の OS コマンドインジェクションの脆弱性	8.3	8.8	2020/2/19	5,022
17	JVNDB-2019-000075	WordPress 用プラグイン Custom Body Class における複数の脆弱性	2.6	6.1	2019/12/12	4,914
18	JVNDB-2019-000024	Android アプリ「クリエイトＳＤ公式アプリ」におけるアクセス制限不備の脆弱性	2.6	3.3	2019/5/10	4,843
19	JVNDB-2019-009884	FON がオープンリゾルバとして機能してしまう問題	5.0	5.8	2019/10/2	4,839
20	JVNDB-2020-000013	ウイルスバスター クラウド (Windows 版) におけるサービス運用妨害 (DoS) の脆弱性	2.1	6.2	2020/2/14	4,835

表 3-2 は国内の製品開発者から収集した脆弱性対策情報でアクセスの多かった上位５件を示しています。

表 3-2. 国内の製品開発者から収集した脆弱性対策情報へのアクセス上位 5 件 [2020 年 1 月～2020 年 3 月]

順位	ID	タイトル	CVSSv2 基本値	CVSSv3 基本値	公開日	アクセス数
1	JVNDB-2019-013271	Hitachi Automation Director における複数の脆弱性	なし	なし	2019/12/24	5,975
2	JVNDB-2019-013273	Hitachi Compute Systems Manager における DoS 脆弱性	なし	なし	2019/12/24	5,732
3	JVNDB-2019-013272	Hitachi Command Suite 製品および Hitachi Infrastructure Analytics Advisor における複数の脆弱性	なし	なし	2019/12/24	5,407
4	JVNDB-2019-011486	Hitachi Command Suite 製品における不当にファイルが削除される脆弱性	なし	なし	2019/11/11	4,226
5	JVNDB-2018-010027	JP1/Operations Analytics におけるディレクトリパーミッションの問題	3.5	4.9	2018/12/4	4,203

注 1）CVSSv2 基本値の深刻度による色分け

CVSS 基本値=0.0～3.9 深刻度=レベル I（注意）	CVSS 基本値=4.0～6.9 深刻度=レベル II（警告）	CVSS 基本値=7.0～10.0 深刻度=レベル III（危険）

注 2）CVSSv3 基本値の深刻度による色分け

CVSS 基本値=0.1～3.9 深刻度=注意	CVSS 基本値=4.0～6.9 深刻度=警告	CVSS 基本値=7.0～8.9 深刻度=重要	CVSS 基本値=9.0～10.0 深刻度=緊急

注 3）公開日の年による色分け

2018 年以前の公開	2019 年の公開	2020 年の公開